Access Control Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this policy is to provide a framework to ensure that access to Superhawk AI assets is provided in a controlled manner based on business and information security requirements.

The framework is designed to ensure that appropriate controls for access management are established to protect Superhawk AI assets from security threats arising from unauthorized access.

2. Scope

This policy applies to all Superhawk AI employees, contractors, and third-party administrators who require access to systems, services, and data used to deliver Superhawk AI's SaaS product. It covers cloud-hosted infrastructure and services on AWS and GCP, code repositories in GitHub, corporate email and identity in Google Workspace, and employee devices (laptops/workstations) that access or store PII, business/operational data, or behavioral data.

3. Policy Statement

Centralized access control is key to ensuring that the correct Superhawk AI staff members access the correct data and systems at the correct level. The principle of least privilege guides Superhawk AI's access controls. These controls apply to information and information processing systems at the application and operating system layers, including networks and network services.

The confidentiality, integrity, and availability of information stored within the information system of Superhawk AI shall be assured by ensuring that only authorized users have access to specific information assets as needed for their business activities.

4. Access Control Policy

4.1 Requirement for Access Control

- Every organization possesses information and information assets that need to be protected from unauthorized use.
- A list of critical systems within Superhawk AI that host services or sensitive data shall be identified and documented. At a minimum, this list shall include AWS and GCP production environments, GitHub repositories containing source code or secrets, Google Workspace administrative accounts, and any third-party SaaS services that process customer PII or behavioral data.
- It is the responsibility of the Information Security Officer to ensure all such systems used to meet business requirements at Superhawk AI are identified, and the list of critical systems is kept updated.

4.2 Access Management

4.2.1 Access Provisioning

- Superhawk AI shall provide access privileges to its systems based on the following principles:
    - Need to know – users or resources shall be granted access to systems that are necessary to fulfill their roles and responsibilities.
    - Least privilege – users or resources shall be given minimum privileges necessary to fulfill their roles and responsibilities.
    - Separation of duties – the practice of ensuring responsibility to perform critical actions is distributed among different individuals to keep a single individual from subverting the process.
- The minimum requirements for access control are to be achieved using one or both of the following methodologies:
    - Role-based Access control: This methodology restricts access to systems and resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users.
    - Rule-based access control: This involves a formal registration and de-registration process for individual users where access is provided based on requests and approvals from authorized personnel.
- For Role-based access Control:
    - Access to information systems and services is managed through role mappings in GitHub (for repository access), Google Workspace (for corporate identity and group membership), and cloud IAM in AWS and GCP for infrastructure access. System administrators maintain role definitions and role-to-system mappings.
    - The roles that may access each critical system shall be identified and documented.
    - By default, staff members are granted access to systems according to their role or team. The ability to grant access to systems is restricted to the administrators of each system.
    - If any access is required outside the defined role matrix, the business justification for such an event must be documented.
- For Rule-based/ Ticket-Based access control:
    - Requests for users' accounts and access privileges must be formally documented and appropriately approved. Access authorization information for a user must be retained for a minimum amount of time as defined in business, contractual, and legal requirements.
    - For any staff member requiring access to systems/platforms/tools, a request needs to be submitted detailing the specific access being requested.
    - The Acceptable Usage Policy needs to be accepted by an employee before being granted access to systems that contain customer data. This policy outlines responsibilities and commitments regarding the acceptable use of Superhawk AI's assets.
    - If a Superhawk AI staff member requires access outside of the default for their role or team, either they or their managers may request additional access to the administrators of the respective systems.
    - When granting such access, it shall be limited to the minimum level required to perform the intended business operation.

4.2.2 Management of Privileged Access Rights

- Superhawk AI operates its access management under the principle of least privilege.
- Privileged access (e.g., cloud console admin, GitHub repo admin, Google Workspace super admin) is restricted to a small set of named administrators. Privileged accounts require multi-factor authentication via Google Workspace and are reviewed quarterly. Temporary elevation of privileges for maintenance or incident response must be approved by the Information Security Officer and documented with a specified expiration.

4.2.3 Management of Passwords and Secret Authentication Information of Users

- It is recommended to minimize the use of passwords wherever possible. Please follow the guidelines to reduce the reliance on passwords:
    - Use a single-sign-on mechanism to authenticate yourself wherever possible. This avoids the need to create new strong passwords. Please ensure that the password/authentication mechanism for the SSO system is secure.
    - Use multi-factor authentication (MFA) techniques to authenticate yourself wherever possible. This adds an additional barrier even if the password is compromised.
- Where passwords are the only way to login to a system, it is recommended to consider the below security requirements:
    - Staff members must use complex passwords, wherever possible, for all of their accounts that have access to critical data. A strong password should consist of at least 8 characters and should contain a combination of alphanumeric + special characters.
    - It is strongly recommended against the reuse of passwords that are or were used elsewhere, e.g., passwords used for personal accounts. A common way attackers obtain access to corporate resources is by using employees' personal passwords that were obtained in breaches of other services.
- Superhawk AI uses Google Workspace as the primary identity provider and encourages SSO wherever supported. Secrets and credentials for applications and infrastructure are stored in approved secret managers (e.g., cloud-native secret manager services in AWS/GCP or an approved secrets management SaaS). Any password or authentication details stored within systems owned and managed by Superhawk AI shall be encrypted at rest and access to secrets is logged and restricted to authorized roles.

4.2.4 Review of Access Rights

- There shall be a periodic reconciliation of user accounts and the associated rights. The reconciliation needs to be performed at least annually.
- Access reviews for critical systems (AWS, GCP, GitHub, Google Workspace) shall be performed at least quarterly. Results of reviews and any remediation actions shall be recorded and retained according to retention requirements.
- It is essential that appropriate actions are taken immediately to remove, disable, or modify any irregularities found in the access reconciliation.

4.2.5 Removal or Adjustment of Access Rights

- Employment termination or change of roles shall trigger relevant processes for revoking or amending access rights.

- On termination or role change, managers must notify IT and administrators to deprovision access in GitHub, Google Workspace, AWS, and GCP within 24 hours. Where accounts are managed by third-party SaaS providers, administrators will follow the provider's deprovisioning processes and document completion.
- The removal or modification of access rights for terminated Superhawk AI employees or contract staff shall be carried out by the relevant administrators.

4.2.6 Secure Log-On Procedures

- Following shall be considered for security when accessing critical systems:
  - If the login is unsuccessful, the error message shall not display which part of the login information was incorrect.
  - Limit the number of unsuccessful log-on attempts.
  - Password shall not be displayed while it is being entered.
  - Multi-factor authentication shall be adopted wherever possible.
  - Using an authentication mechanism like single sign-on (SSO) is also recommended wherever possible.
- Session Time-Out
  - Inactive sessions (Application sessions, Administration Sessions, etc.) shall be shut down where feasible after a defined period of inactivity.
  - Intranet site may be exempted from the requirement of session time-out.
  - Session time-out requirements shall be implemented for all the critical systems as feasible and applicable.
  - Re-authentication may be considered at timed intervals.
- SSO via Google Workspace is the preferred authentication method for corporate services; where native login is required for cloud consoles or third-party tools, MFA is mandatory for privileged and administrative accounts.

4.2.7 Access Monitoring

- For all production infrastructure, logging must be enabled to ensure user accountability is maintained in case of any issues. It is recommended to have additional security measures like an intrusion detection/prevention system to detect any unauthorized access.
- Logging and audit trails for AWS, GCP, GitHub, and Google Workspace shall be enabled and retained according to retention policies. Security-relevant logs are aggregated and reviewed by the security team; alerts for suspicious access patterns are configured in cloud-native monitoring services and any third-party SIEMs if used.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of

employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. The IT/Cloud administrators are responsible for implementing access controls in AWS and GCP. The DevOps and engineering leads are responsible for managing GitHub repository access. HR and hiring managers are responsible for initiating provisioning and deprovisioning requests. All staff members and contractors are responsible for complying with this policy and completing required training and Acceptable Usage acknowledgements. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization or its technology stack (e.g., changes to use of AWS, GCP, GitHub, or Google Workspace).

End of Access Control Policy. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026